

1

REMARKS

2 These remarks follow the order of the paragraphs of the office action. Relevant portions of the
3 office action are shown indented and italicized.

4 ***DETAILED ACTION***
5 ***Response to Amendment***

6 *Applicant's submission filed on 11/14/2006 has been entered. Claims 1,4-5, 10,13-15 and*
7 *20 have been amended. Claims 1-20 are pending in the application.*

8 ***Response to Arguments***

9 *Applicants arguments filed November 14, 2006 have been fully considered but are moot*
10 *in view of the new ground(s) of rejection set forth below. As address below, the claim 'is*
11 *anticipated by S. Ma, et al, "EventMiner: An integrated mining tool for Scalable*
12 *Analysis of Event Data", May 21, 2001, www.reseach.ibm.com, in view of D.*
13 *Kranzlmuller, S. Gradbner. J. Volkert, Event graph visualization for debugging large*
14 *applications", Proc. of the SIGMETRICS symposium on Parallel and distributed tools,*
15 *Philadelphia, PA, United States. Pages: 108-117 (hereinafter Kranzlmuller).*

16 *The cited prior art Ma reference teaches in Fig- 7 and the last paragraph of the Page 12*
17 *plotting the primary attribute (e.g., with the attribute values indicating the troublesome*
18 *hosts having significantly high event counts) versus time with the attribute values for*
19 *events in a communication network and the primary attribute is selected from a plurality*
20 *of attributes related to the one or more significant measurements such as the*
21 *co-occurrences (i.e.. the total number of times that two hosts generate events within a*
22 *predefined time window), the conditional probability of the two hosts (i.e., the probability*
23 *of a host generating an event given the observation hat the other host has generated an*
24 *event), the chi-squared test and so on. Moreover, the Fig. 4 shows the coloring of the*
25 *events having the seconary attribute with the patterns indicating the authentication*
26 *failure and SNMP request in order to differentiate using the coloring the events with*
27 *authentication failure from other events. A pattern label is assigned to lie events falling*
28 *into the same pattern. Finally, the operator can view different event attributes by*
29 *switching menus (Fig. 6). Ma has taught in Fig. 7 and the last paragraph of the Page 12*
30 *plotting the primary attribute (e.g., with the attribute values indicating the troublesome*
31 *hosts having significantly high event counts) versus time with the attribute values for*
32 *events in a communication network. Ma has also taught a plurality of attributes related*
33 *to the one or more significant measurements such as the co-occurrences (i.e., the total*
34 *number of times that two hosts generate events within a predefined time window), the*
35 *conditional probability of the two hosts (i.e., the probability of a host generating an event*
36 *given the observation that the other host has generated an event), the chi-squared test*
37 *and so on wherein the attribute values are plotted in the same plot. It is clear that Ma*

1 discloses attributes including categorical attributes of the hosts, event types, severity of
 2 the events, etc. See Figs. 2, 6, 7 and 9. In Ma many significant event patterns are
 3 simultaneously identified within a single plot without the operator's switching between
 4 the various event attributes. Ma discloses display label to the events such as "Link down
 5 of host A", "node down of host B", 'authentication failure of host A". etc., including the
 6 colors for coloring the different patterns that indicate the attribute values of the primary
 7 attribute such as the co-occurrences of some specific events within a predefined time
 8 window. Ma discloses a secondary display label including the colors for coloring the
 9 different patterns for the events in the communication network that indicate the attribute
 10 values of the primary attribute such as the co-occurrences of some specific events within
 11 a predefined time window. Ma teaches in Fig 5(b) displays two different attributes for the
 12 events: Figs. 2 and 4 show y-axis is the host name attribute as well as the coloring of
 13 attribute such as "authentication failure' events in red and "SNMP request events in
 14 green: therefore, at least two event attributes such as host name, authentication failure,
 15 SNMP request have been simultaneously monitored in the plot of Figs. 2 and 4. The
 16 menu options shown in Fig. 6 allow for the y-axis attribute mappings be changed.
 17 Moreover, Ma teaches mapping a plurality of attributes to item and viewing both
 18 numerical attribute and categorical attribute on a same plot in Fig. 7 (See Page 10).
 19 Thus, Ma at least teaches or suggests the claim limitation of viewing a secondary
 20 attribute of said each event together with the primary attribute on said display. Ma is
 21 silent to "automatically generating a large variety of visualizations along other attribute
 22 axes, and identifying correlations by superimposing and cross-referencing these
 23 visualizations". However, Kranzlmuller teaches the claim limitation of "automatically
 24 generating a large variety of visualizations along other attribute axes, and identifying
 25 correlations by superimposing and cross-referencing these visualizations." Kranzlmuller
 26 teaches automatically generating a large variety of visualizations (P0- P7) along the
 27 other attribute axes (See Kranzlmuller Page 109 and Figs. 1-2 showing the
 28 arrangement of the axes applied to the visualization of the event graph wherein a
 29 plurality of visualizations for dimensions P0-P7 are superimposed in the event graph)
 30 and identifying correlations (such as the inter-process dependencies between processes
 31 among the event visualizations wherein dependencies among me processes mean
 32 correlations among the processes in the event visualizations) by superimposing (the
 33 processes/dimensions P0-P7 are superimposed vertically wherein the events belonging
 34 to the dimensions P0-P7 are plotted with the attribute values of the events or
 35 dimension values being allocated to each of the processes/dimensions P0-F7 and the
 36 attribute values for example are the colors which are changed to indicate the state of
 37 the process in the value range of (active, idle, blocked); see Page 109 and therefore the
 38 y-axis presents the attribute values allocated to each of the processes/dimensions
 39 P0-F7) and cross-referencing (e.g. the inter-process dependencies between processes,
 40 e.g., directed edges between vertices are either communication or sequential program
 41 flow and the events/ti and/ti occur in process P0, Event B1-B3 occurs in process P1. In
 42 process 1 the event B1 has the attribute of being the send event and A1 has the
 43 attribute of being the receive event. The send event B1 and the receive event A1 is
 44 connected through a directed arc in the graph. The process axis is arranged vertically)
 45 these visualizations. Kranzlmuller teaches viewing a plurality of attributes P0-F7 for

1 *the visualizations of the events in a communication network. Kranzlmuller teaches*
2 *viewing a secondary categorical attribute (e.g., an event belonging to the category P0)*
3 *of said each event together with the primary categorical attribute (e.g., an event*
4 *belonging to the category P1) on said display (See Page 109, Fig. 2). It would have*
5 *been obvious to one of the ordinary skill in the art at the time the invention was made to*
6 *have incorporated Kranzlmuller's teaching into Ma to view a plurality of attributes*
7 *related to the events on the same display because Ma at least suggests the claim*
8 *limitation of viewing a secondary attribute of said each event together with the primary*
9 *attribute on said display at least by the means of mapping of the secondary attribute and*
10 *coloring the secondary attribute and therefore the secondary attribute and the primary*
11 *attribute are distinctly viewed (See Figs. 2 and 4 of Ma wherein a plurality of secondary*
12 *attributes are colored so as to be viewed. Although the menu options are used in Fig. 6 of*
13 *Ma to switch the primary attribute to the another attribute the secondary attribute can be*
14 *viewed by the coloring mechanism as disclosed and can be further queried and displayed*
15 *in different plots on the same display). One of the ordinary skill in the art would have*
16 *been motivated to do so such that the inter-process dependency among events and event*
17 *categorical attributes are visualized (Kranzlmuller Page 109).*

18 In response, the applicants continue to respectfully states that applicants continue to take
19 exception to the allegation that the presently claimed invention is anticipated by Ma in view of
20 Kranzlmuller. However, further amendments are made to the claims herewith, in order to bring
21 this application to allowance quickly.

22 ***Claim Rejections -35 USC §101***

23 *35 U.S.C. 101 reads as follows:*

24 *Whoever invents or discovers any new and useful process, machine, manufacture, or*
25 *composition of matter, or any new and useful improvement thereof, may obtain a patent*
26 *therefor, subject to the conditions and requirements of this title.*

27 ***Claim 10:*** *Claim 10 recites "computer readable program on tangible computer media".*
28 *The claimed tangible computer media is not necessarily a computer readable medium.*
29 *The claimed computer readable program is not necessarily computer executable*
30 *instructions, There is no structural and functional interrelationship between the*
31 *instructions and the rest of the computer to permit the instructions' functionality to be*
32 *realized. Claim 10 is, thus, non-statutory.*

33 In response, the applicants continue to respectfully states that claim 10 is amended to show that it
34 is a computer readable program on tangible computer readable medium and being computer

1 executable instructions. This overcomes the rejection of claim 10 under 35 USC §101, and claim
2 10 is allowable.

3 *Claim 11: Claim 11 recites “a computer program on a computer readable medium
4 containing a program code to carry out all steps of the method of claim 1”. The claimed
5 computer program is not necessarily computer executable instructions, There is no
6 structural and functional interrelationship between the instructions and the rest of the
7 computer to permit the instructions’ functionality to be realized by the computer. Claim
8 11 is, thus, non-statutory.*

9 In response, the applicants continue to respectfully states that claim 11 is amended to show that
10 the program code being computer executable instructions. This overcomes the rejection of claim
11 11 under 35 USC §101, and claim 11 is allowable.

12 ***Claim Rejections -35 USC §112***

13 *The following is a quotation of the first paragraph of 35 U.S.C. 112: The specification
14 shall contain a written description of the invention, and of the manner and process of
15 making and using it, in such full, clear, concise, and exact terms as to enable any person
16 skilled in the art to which it pertains or with which it is most nearly connected, to make
17 and use the same and shall set forth the best mode contemplated by the inventor of
18 carrying out his invention.*

19 *Claims 1-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with
20 the written description requirement. The claim(s) contains subject matter which was not
21 described in the specification in such a way as to reasonably convey to one skilled in the
22 relevant art that the inventor(s), at the time the application was filed, had possession of
23 the claimed invention. For example, the claim 1 recites “automatically generating a
24 large variety of visualizations along other attribute axes, and identifying correlations by
25 superimposing and cross-referencing these visualizations.” By the claim limitations, the
26 visualizations are generated along **other attribute axes**. However, lines 7-11 of the claim
27 1 refer the x-axis and y-axis as attribute axes. it is understood from the claim limitations
28 set forth in the claim 1 that other attribute axes as claimed are the axes other than the
29 x-axis and y-axis, See also Fig. 1 of applicant’s specification. However, the axes as
30 claimed other than the x-axis and y-axis set forth in lines 7-11 of the claim are not
31 disclosed in applicant’s specification. The applicant’s specification (e.g., Fig. 1) shows
32 that the visualizations are superimposed and cross-referenced along the y-axis with
33 respect to the x-axis, There are no other axes involved in these visualizations. Therefore,
34 the metes and bounds of the coverage of ‘at least base claim 1 cannot be ascertained. To
35 comply with the “written description” requirement of 35 U.S.C. 112, first paragraph, an
36 applicant must convey with reasonable clarity to those skilled in the art that, as of the
37 filling date sought, he or she was in possession of the invention. The invention is, for*

purposes of the "written description" inquiry, whatever is now claimed. Vas-Cath, Inc. v. Mahurkar, 935 F.2d 1555, 1563-64, 19 USPQ2d 1111, 1117 (Fed. Cir. 1991). For purposes of written description, one shows "possession" by descriptive means such as words, structures, figures, diagrams, and formulas that fully set forth the claimed invention. Lockwood v. American Airlines, Inc., 107 F.3d 1565, 1572, 41 USPQ2d 1961, 1966 (Fed. Cir. 1997). Such descriptive means cannot be found in the disclosure for the inventions of the claim 1.

The claims 1-13, and 15-19 depend upon the claim 1 and are rejected due to their dependency on the claim 1.

10 In response, the applicants continue to respectfully states that claim 1 is amended to make it more
11 clear and to better protect the invention. The last step, namely:

12 automatically generating a large variety of visualizations along other attribute axes, and
13 identifying correlations by superimposing and cross-referencing these visualizations
14 is deleted. This overcomes the rejection of claims 1-13 and 15-19 under 35 USC §112, and
15 claims 1-13 and 15-19 are allowable.

16 The office communication further states:

The claims 14 and 20 are subject to the same rationale of rejection set forth in the claim 1.

19 In response, the applicants continue to respectfully states that claims 14 and 20 are amended to
20 make each more clear and to better protect the invention. The last step, namely:

automatically generating a large variety of visualizations along other attribute axes, and identifying correlations by superimposing and cross-referencing these visualizations is deleted. This overcomes the rejection of claims 14 and 20 under 35 USC §112, and claims 1 and 20 are allowable.

Claim Rejections -35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112: The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 14 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 14 recites the limitation "the machine" in line 2 of the claim. There is insufficient antecedent basis for this limitation in the claim.

5 In response, the applicants continue to respectfully states that claim 14 is amended so that the
6 words 'the machine' are replaced by the words 'a computer.' This overcomes the rejection of claim
7 14 under 35 USC §112, and claim 14 is allowable.

Claim Rejections -35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over S. Ma, et al., "EventMiner: An integrated mining tool for Scalable Analysis of Event Data", May 21, 2001 www.research.ibm.com in view of D. Kranzmuller, S. Gradbner, J. Volkert, "Event graph visualization for debugging large applications", Proc. of the SIGMETRICS symposium on Parallel and distributed tools, Philadelphia, PA, United States, Pages: 108-117 (hereinafter Kranzmuller).

23 In response, the applicants respectfully state that Claims 1-20 are apparently not made obvious by
24 the combined art references to S. Ma, et al., and Kranzlmuller. Applicants respectfully state that
25 continued exception is taken with the so called equivalencies of elements in Claims 1-20 and the
26 cited art, as stated previously. This is particularly in regard to use of words in claims 1-20 of
27 ‘attributes’, ‘primary’, ‘events’, ‘display label’ etc. Further exception is taken with the so called
28 equivalencies of elements in Claims 1-20 and the combined art. The present invention, claimed in
29 Claims 1-20, is for:

"Monitoring events triggered by a computer network. Each event being provided with attribute values allocated to a given set of attributes, and providing an event display, determining a primary attribute and a corresponding display label of the events selected

1 from the given set of attributes presented with attribute values on a cross plot, providing a
2 pattern algorithm to detect whether an arrived event is part of a given pattern, providing a
3 mapping algorithm to map attribute values on the cross plot, allocating a second display
4 label to the events indicating the attributes uncovered as part of the given pattern, plotting
5 events arriving and including an attribute value allocated to a primary attribute into the
6 cross plot, and plotting events arriving within the time period and detected by the pattern
7 algorithm as part of the given pattern into the cross plot with the second display label
8 indicating the given pattern."

9 The cited document of S. Ma, et al, Dated: May 21, 2001, is entitled: "EventMiner: An
10 integrated mining tool for Scalable Analysis of Event Data". The Ma abstract reads :
11 "Exploring large data sets typically involves activities that interwoven the following:
12 querying databases, mining the results returned, and visualizing both the raw data and the
13 parterres discovered. This interweaving of functions arises both from the semantics of
14 what the analyst hopes to achieve and from salability requirements for dealing with large
15 data volumes. Herein is described a tool, EventMiner, that integrates querying mining ,
16 and visualization so as to better analyze temporal data. We discuss the novel visualization
17 techniques employed such as visualizing the results of data mining. Also, we address the
18 large scale visualization of categorical data and how intelligent ordering of data can aid in
19 this task. Though out, we illustrate the capabilities of EventMiner by applying it to event
20 data from large computer networks.

21 Thus Ma is concerned with mapping events that have been queries from a database along the
22 temporal axis, i.e. In the order in which they were presumably received, or recorded. Ma
23 recognizes that time is only one possible visualization axis however does not offer any
24 alternatives, nor gives indication of the potential use or usefulness of any other axis. Ma is
25 primarily concerned with abstracting data from large volume to abstract visual representations.

26 Ma is not concerned with visualizing data that are being received from sensors directly, i.e.
27 without intermediate storage in a database, and, even more importantly, is not concerned with

1 visualizing the data along primary or secondary attribute axis, as in claims 1-20. In this present
2 patent we believe the value of the visualization does not come from the abstraction that Ma offers,
3 but by automatically generating a large variety of visualizations along many different attribute
4 axis, and identifying correlations etc., by superimposing and cross-referencign these
5 visualiationsas in claims 1-20.

6 The other cited document of D. Kranzlmuller, S. Gradbner, J. Volkert, is entitled: "Eventgraph
7 visualization for debugging large applications". The Kranzlmuller abstract reads :

8 "Software repair and performance tuning of parallel programs are two difficult tasks in
9 the parallel software lifecycle. The difficulties are further increased, if the target system is
10 a parallel machine executing a program with many processes on a large amount of data.
11 The existing debugging tools attack this problem with different approaches concerning
12 monitoring and visualization techniques. The event graph visualization or space-time
13 diagram is only one possibility to perform the analysis, but it is included by many existing
14 tools.

15 An example for usage of the event graph is ATEMPT, A Tool for Event
16 ManiPulaTion. The functionality for error debugging (errors in the communication
17 structure, race conditions) and for performance analysis (bottlenecks through blocking
18 communication) is bated on this global communication graph. Extensions to the regular
19 visualization are the abstraction mechanisms provided by ATEMPT. Through horizontal
20 and vertical abstraction the event graph can be used to debug even large applications. The
21 key relies on reducing the visualized information of data that are important for error
22 detection and performance tuning."

23 Thus Kranzlmuller is concerned with the abstraction of large data volumes into smaller sets that
24 can be visulatized effectively. Kranzlmuller is not concerned with generating a variety of views
25 onto the data set, along different attribute axis, without abstraction or reduction, as in claims
26 1-20. There is apparently no reason to combine Ma with Kranzlmuller except in an attempt to
27 find elements of claims 1-20 using hindsight. This is not allowed. Besides even the combination
28 does not make claims 1-20 obvious.

1 Most particularly, besides the differences stated in previous responses, the combined art is not
2 concerned with superimposing and cross-referencing different visualizations of the same data, as
3 in claims 1-20. Combining Kranzlmuller with Ma does not overcome the argument made in
4 previous responses and in this response. Thus claims 1-20 are allowable over the cited combined
5 art.

6 *Claim 1: Ma teaches a method of monitoring events in a computer network, the method
7 comprising: Said computer network triggering said events, each event being provided
8 with attribute values allocated to a given set of attributes of said each event (The term
9 attributes “at clear as it may be related to the data object attributes for each event or the
10 pattern attributes for each pattern for a plurality of data objects; However, the pattern
11 attributes for a plurality of data objects are also related to the data object attributes as a
12 pattern is computed from the plurality of data objects. The cited reference teach mapping
13 a plurality of data attributes to item to identify correlations across different hosts and
14 event types by using the mapping that maps the pair of event type and host name to item
15 and leaves key empty. See Page 11. Moreover, the cited reference in Page 1, second
16 paragraph, explicitly teaches the attribute values, see the last paragraph of Page 6 and
17 the first and second paragraphs of Page 8, the last paragraph of Page 12, and the real
18 data set collected from a production computer network containing thousands of managed
19 nodes including routers, hubs and servers are described in the last paragraph of page 3
20 and identifying unknown event patterns that can be used for real-time monitoring is
21 described in the second paragraph of page 3. Ma has also taught a plurality of pattern
22 attributes related to the one or more significant measurements such as the
23 co-occurrences, i.e., the total number of times that two hosts generate events within a
24 predefined time window, the conditional probability of the two hosts, i.e., the probability
25 of a host generating an event given the observation that the other host has generated an
26 event, the chi -squared test and so on); Simultaneously monitoring various event
27 attributes versus the arrival time of said events (e.g., Fig. 5(b) displays two different
28 attributes for the events; Figs. 2 and 4 show y-axis is the host name attribute as well as
29 the coloring of attribute such as “authentication failure events in red and “SNMP
30 request events in green: therefore, at least two event attributes such as host name,
31 authentication failure. SNMP request have been simultaneously monitored in the plot of
32 Figs. 2 and 4); Providing an event display with a cross plot having x and y coordinate
33 axes, the x-axis presenting a time period and the y-axis present an attribute value range
34 (e.g., The cited reference teach mapping a plurality of data attributes to item to identify
35 correlations across different hosts and event types by using the mapping that maps the
36 pair of event type and host name to item and leaves key empty. See Page 11, Figs. 2,4,6
37 7, 9 and the third paragraph of Page 8 describes a scatter plot or cross plot having an
38 y-axis representing around 160 hosts of a communication network and the x axis has
39 been described in the figures as well as the first paragraph of page 6; for attribute value
40 range, see these figures as well as the description in the second paragraph of Page 8);*

1 Determining a primary attribute of the events selected from the given set of attributes to
2 be presented with its attribute values on the y-axis of the cross plot (e.g., The cited
3 reference teach mapping a plurality of data attributes to item to identify correlations
4 across different hosts and event types by using the mapping that maps the pair of event
5 type and host name to item and leaves key empty. The attributes including the categorical
6 attributes or temporal attributes and the primary attribute values are displayed in Figs.
7 2,4,6 and 7 and multiple attributes are described in the last paragraphs of Page 11 and
8 12). Allocating a first display label (e.g., one of the colors indicating the patterns such as
9 the Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the
10 cross plot of Figs. 2, 6 and 9 such as “Link down of host A “ and “node down of host
11 B”) to the events (e.g., alarms in Page 10) indicating (mapping of the attributes wherein
12 the mapping results are shown in the plots with the patterns identifying/indicating the
13 attribute values of the primary attribute related to the categorical attribute such as the
14 host A or the host B. Moreover, the pattern attribute values identifying the pattern 1 and
15 the pattern 2 also describe the primary attribute such as the host A and the host B for the
16 patterns such as “Link down of host A” and “node down of host B”) the attribute values
17 of the primary attribute (e.g., co-occurrence of certain events or the categorical attribute
18 and event type associated with the events wherein the primary attribute is related to the
19 primary attribute of the data set or the primary attribute of the patterns; See Page 12 and
20 the key attribute values are described in the second paragraph of page 3), providing a
21 pattern algorithm (the pattern algorithm is described in Fig. 7 as well as the mining
22 algorithm as described in the last paragraph of page 12 or the EventMiner for ordering
23 categorical values wherein the event generating, say every 300 seconds, may be
24 identified) to detect whether an arrived event (arrived event are the selected event objects
25 or the selected data objects in a specific time range related to the events progressively
26 loaded from a database or the mining alarm logs in a ‘cal tune system; see first
27 paragraph of page 13 and the last paragraph of page 10 and a new query that retrieves
28 the relevant data objects for more analysis in which a new query is restricted to a range
29 constraint for a numerical attribute; see the last paragraph of page 10) is part of the
30 given pattern (is part of the given pattern such as the Pattern 1 or the Pattern 2 from the
31 identifiable patterns such as the **SNMP request, authentication failure, link up, link**
32 **down, port up, port down** wherein authentication failure indicates a possible security
33 **intrusion and link down of host A indicates the attribute associated with the data**
34 **objects as well as the attribute associated with the event**) on the basis of a comparison of
35 the attributes allocated to the given pattern and of the attributes assigned to the arrived
36 event (e.g., the CO-occurrence measurements for events can be computed for the data
37 sets or the data objects and the temporal correlation with the selected hosts from the
38 other side of the AttributeViewer can be identified using the color linkage by the coloring
39 and filtering algorithm or the data mining algorithm in which the difference or similarity
40 in terms of patterns indicated by colors is compared; see page 12-13), providing a
41 mapping algorithm to map any attribute value of an attribute selected from the given set
42 of attributes onto the y-axis of the cross plot (see the last paragraphs of Page 11-12; The
43 cited reference teach mapping a plurality of data attributes to item to identify
44 correlations across different hosts and event types by using the mapping that maps the
45 pair of event type and host name to item and leaves key empty.). Allocating a second

1 display label (e.g., one of the colors indicating the patterns such as the Pattern 1, Pattern
2 2, Pattern 3 and Pattern 4 as marked in the scatter plot or the cross plot of Figs. 2, 6, 7;
3 SNMP request, authentication failure, link up, link down, port up, port down wherein
4 authentication failure indicates a possible security intrusion may be used as display
5 labels as well. The attribute values may be used as display labels as well) to the events
6 indicating the attribute values of the attributes being uncovered (discovered) as part of
7 the given pattern (e.g., the co-occurrence measurements for events can be computed and
8 the temporal correlation with the selected hosts from the other side of the AttributeViewer
9 can be identified using the color linkage by the coloring and filtering algorithm or the
10 data mining algorithm in which the difference or similarity in terms of patterns indicated
11 by colors is compared; see page 12-13; the display labels indicate the attribute values of
12 the attributes being discovered as part of the given pattern, for example, the second host
13 was near a critical level for a key metric indicates the attribute values of the attributes
14 being discovered as part of the given pattern), plotting all the events arrived within the
15 time period and including an attribute value allocated to the primary attribute into the
16 cross plot with the first display label indicating the primary attribute, the position of the
17 first display label of each event in the cross plot being determined on the basis of the
18 attribute value of the primary attribute of the event and its arrival time (e.g., The cited
19 reference teach mapping a plurality of data attributes to item to identify correlations
20 across different hosts and event types by using the mapping that maps the pair of event
21 type and host name to item and leaves key empty. Figs. 2, 4, 6, and 7 and the related
22 paragraphs mentioned above in "allocating a first display label". e.g. one of the colors
23 indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3 and Pattern 4 as
24 marked in the scatter plot or the cross plot of Figs 2, 6, 7; SNMP request, authentication
25 failure, link up, link down, port up, port down wherein authentication failure indicates a
26 possible security intrusion may be used as display labels as well. The attribute values
27 maybe used as display labels as well), and Plotting the all events arrived within the time
28 period (Figs. 2, 4, 6, and 7 plot the all events within a specific time range) and being
29 detected by means of the pattern algorithm (by the event miner algorithm) as part of the
30 given pattern into the cross plot with the second display label (e.g., one of the colors
31 indicating the patterns such as the Pattern 1, Pattern 2, Pattern 3 and Patter,: 4 as
32 marked in the scatter plot or the cross plot of Figs. 2,6, 7 and 9 or Pattern 2 or the Green
33 Spike in Fig. .10), the position of the second display label of each event in the cross plot
34 being determined by the mapping algorithm on the basis of the attribute value of the
35 attribute of the event (see Figs. 1-10) on the basis of the attribute value of the attribute of
36 the event being uncovered (uncovered for example in the alarm log and uncovered by the
37 mining algorithm) as part of the given pattern and its arrival time (discovered as part of
38 the given pattern such as Patterns 1-4 and its arrival time; all the selected events are in a
39 specific time range as plotted in Figs. 2, 4, 6, 7 and 10). In other words, Ma discloses an
40 apparatus and system for monitoring events in a computer network enabling an operator
41 of an intrusion-detection system to simultaneously monitor various event attributes versus
42 the arrival time of the events, for example, authentication failure indicates a possible
43 security intrusion may be used as display labels. The cited prior art teaches in Fig. 7 end
44 the last paragraph of the Page 12 plotting the primary attribute (e.g., with the attribute
45 values indicating the troublesome hosts having significantly high event counts) versus

1 time with the attribute values for events in a communication network and the primary
2 attribute for a host is selected from a plurality of attributes related to the categorical
3 values, the one or more significant measurements such as the co-occurrences (i.e., the
4 total number of times that two hosts generate events within a predefined time window),
5 the conditional probability of the two hosts (i.e., the probability of a host generating an
6 event given the observation that the other host has generated an event), the chi-squared
7 test and so on. Fig. 4 shows the coloring of the events having the primary attribute with
8 the patterns indicating the authentication failure and SNMP request in order to
9 differentiate using the coloring the events with authentication failure from other events, A
10 pattern label is assigned to the events falling into the same pattern. Finally, the operator
11 can view different event attributes by switching menus (Fig. 6). Ma has taught in Fig. 7
12 and the last paragraph of the Page 12 plotting the primary attribute (e.g., with the
13 attribute values indicating the troublesome hosts having significantly high event counts)
14 versus time with the attribute values for events in a communication network. Ma has also
15 taught a plurality of attributes related to the one or more significant measurements such
16 as the co-occurrences (i.e., the total number of times that two hosts generate events
17 within a predefined time window), the conditional probability of the two hosts (i.e., the
18 probability of a host generating an event given the observation that the other host has
19 generated an event) the chi-squared test and so on wherein the attribute values are
20 plotted in the same plot. See Figs. 2,6, 7 and 9. Many significant event patterns are
21 simultaneously identified within a single plot without the operator's switching between
22 the various event attributes. Ma discloses display label including the colors for coloring
23 the different patterns that indicate the attribute values of the primary attribute such as
24 the co-occurrences of some specific events within a predefined time window. Ma teaches
25 in Fig. 5(b) displays two different attributes for the events; Figs. 2 and 4 show y-axis is
26 the host name attribute as well as the coloring of attribute such as "authentication
27 failure" events in red and "SNMP request events in green, therefore, at least two event
28 attributes such as host name authentication failure. SNMP request have been
29 simultaneously monitored in the plot of Figs. 2 and 4. The menu options shown in Fig. 6
30 allow for the y-axis attribute mappings be changed. Moreover, Ma teaches mapping a
31 plurality of attributes to item and viewing both numerical attribute and categorical
32 attribute on a same plot in Fig. 7 (See Page 10). Thus, Ma at least teaches or suggests
33 the claim limitation of viewing a secondary attribute of said each event together with the
34 primary attribute on said display, Ma is silent to automatically generating a large variety
35 of visualizations along other attribute axes, and identifying correlations by
36 superimposing and cross-referencing these "visualizations." However, Kranzlmuller
37 teaches the claim limitation of "automatically generating a large variety of visualizations
38 along other attribute axes, anti identifying correlations by superimposing and
39 cross-referencing these visualizations." Kranzlmuller teaches automatically generating a
40 large variety of visualizations (F0-P7) along the other attribute axes (See Kranzlmuller
41 Page 109 and Figs. 1-2 showing the arrangement of the axes applied to the visualization
42 of the event graph wherein a plurality of visualizations for dimensions P0-P7 are
43 superimposed in the event graph) and identifying correlations (such as the inter-process
44 dependencies between processes among the event visualizations wherein dependencies
45 among the processes mean correlations among the processes in the event visualizations)

1 by superimposing (the processes/ dimensions P0-P7 are superimposed vertically wherein
2 the events belonging to the dimensions P0-P7 are plotted with the attribute values of the
3 events or dimension values being allocated to each of the processes/dimensions P0-P7
4 and the attribute values for example are the colors which are changed to indicate the
5 state of the process in the value range of (active, idle, blocked); see Page 109 and
6 therefore the y-axis presents the attribute values allocated to each of the
7 processes/dimensions P0-P7) and cross-referencing (e.g., the inter-process dependencies
8 between processes, e.g., directed edges between vertices are either communication or
9 sequential program flow and the events A1 and A1 occur in process P0, Event B1-B3
10 occurs in process P1. In process 1 the event B1 has the attribute of being the send event
11 and A1 has the attribute of being the receive event. The send event B1 and the receive
12 event A is connected through a directed arc in the graph. The process axis is arranged
13 vertically) these visualizations. Kranzlmuller teaches viewing a plurality of attributes
14 P0-P7 for the visualizations of the events in a communication network. Kranzlmuller
15 teaches viewing a secondary categorical attribute (e.g., an event belonging to the
16 category P0) of said each event together with the primary categorical attribute (e.g., an
17 event belonging to the category P1) on said display (See Page 109, Fig. 2). It would have
18 been obvious to one of the ordinary skill in the art at the time the invention was made to
19 have incorporated Kranzlmuller's teaching into Ma to view a plurality of attributes
20 related to the events on the same display because Ma at least suggests the claim
21 limitation of viewing a secondary attribute of said each event together with the primary
22 attribute on said display at least by the means of mapping of the secondary attribute and
23 coloring the secondary attribute and therefore the secondary attribute and the primary
24 attribute are distinctly viewed (See Figs. 2 and 4 of Ma wherein a plurality of secondary
25 attributes are colored so as to be viewed. Although the menu options are used in Fig. 6 of
26 Ma to switch the primary attribute to the another attribute, the secondary attribute can
27 be viewed by the coloring mechanism as disclosed and can be further queried and
28 displayed in different plots on the same display). One of the ordinary skill in the art
29 would have been motivated to do so such that the inter-process dependency among events
30 and event categorical attributes are visualized (Kranzlmuller Page 109).

31 In response, the applicants respectfully state that the combined art of Ma and Kranzlmuller
32 apparently do not make claim 1 obvious. Claim 1 as further amended now reads:

33 1. A method comprising monitoring network activities as a time-ordered sequence of
34 events in a computer network, each event having attributes triggered by an
35 intrusion-detection system, each event being characterized by a given set of attributes
36 called dimensions, each event forming an n-dimensional space, the step of monitoring
37 comprising:

1 said computer network triggering said events, each event being provided with attribute
2 values allocated to a given set of attributes of said each event, each attribute having a
3 particular attribute value,

4 simultaneously monitoring each particular attribute value of various event attributes from
5 said given set of attributes versus the arrival time of said each event,

6 providing an event display with a cross plot having x and y coordinate axes, the x-axis
7 presenting a time period and the y-axis presenting an attribute value range, and visualizing
8 data along said x and y coordinate axes, said axes being attribute axes,

9 determining a primary attribute of said each event, said primary attribute being selected
10 from the given set of attributes, each said primary attribute of said each event to be
11 presented with a corresponding attribute value on the y-axis of the cross plot,

12 allocating a first display label to the events indicating the attribute value of the primary
13 attribute of each event, providing a pattern algorithm to detect whether an arrived event is
14 part of the given pattern on the basis of a comparison of the attributes allocated to the
15 given pattern and of the attributes assigned to the arrived event, providing a mapping
16 algorithm to map any attribute value of an attribute selected from the given set of
17 attributes onto the y-axis of the cross plot,

19 allocating a second display label to said each event indicating the attribute values of the
20 attributes being uncovered as part of the given pattern,

21 plotting all events that arrived within the time period and including an attribute value
22 allocated to the primary attribute into the cross plot with the first display label indicating
23 the primary attribute, the position of the first display label of said each event in the cross
24 plot being determined on the basis of the attribute value of the primary attribute of the
25 event and its arrival time,

1 plotting all events that arrived within the time period and being detected by means of the
2 pattern algorithm as part of the given pattern into the cross plot with the second display
3 label indicating the given pattern, the position of the second display label of said each
4 event in the cross plot being determined by the mapping algorithm on the basis of the
5 attribute value of the attribute of the event being uncovered as part of the given pattern
6 and its arrival time,

7 viewing a secondary attribute of said each event together with the primary attribute on
8 said display.

9 The applicant continue to respectfully take particular exception with the alleged equivalency of
10 elements in claim 1 and the cited art, and take exception with the Examiner assertions.

11 In addition, to the previous exceptions, the additional amendment to claim 1 further makes it
12 allowable over the prior art. The combined art. does not anticipate or make obvious:

13 monitoring network activities as a time-ordered sequence of events in a computer
14 network, each event having attributes triggered by an intrusion-detection system, each
15 event being characterized by a given set of attributes called dimensions, each event
16 forming an n-dimensional space,

17 which is now in claim 1. Neither is concerned with intrusion-detection or an intrusion-detection
18 system. Neither is apparently concerned with event being characterized by a given set of
19 attributes called dimensions, each event forming an n-dimensional space.

20 As previously stated, claim 1 shows that the attribute are event attributes, and to show explicitly
21 that it includes “simultaneously monitoring various event attributes versus the arrival time of each
22 the events,” and to specifically add a step of “viewing a secondary attribute of said each event
23 together with the primary attribute on said display.” This apparently more clearly distinguishes
24 claim 1 from the cited reference. Thus claim 1 and all claims that depend thereupon are allowable
25 over Ma.

1 Claim 1- 20 state that the value of the visualization is derived from generating multiple
2 visualizations along different attributes and using those to identify interesting event patterns by
3 superposition and cross-referencing.

4 A review of Ma and Kranzlmuller show that even the combination does not do or allude to the
5 steps of claim 1. The combination does not do the steps of automatic generation of multiple
6 visualizations and providing means for cross-referencing. Thus the combined art does not make
7 claim 1 obvious, and claim 1 and all claims depending on claim 1 are allowable.

8 *Re Claims 2-3: Ma further discloses selecting the new events within the specified time
9 period and plotting the new events within the shifted time period into the cross plot. See
10 Figs. 6,7,9 and 10 in which events in the two time periods are drawn and the spikes are
11 identified and the newly selected events are redrawn as determined by the data mining
12 algorithm for the time period during which the new events are retrieved. The database
13 records the attribute values and the arrival time of a new event, The pattern algorithm
14 determines on the basis of the recorded attribute values of event whether or not the newly
15 arrived event in the database and the newly retrieved event from the database includes an
16 attribute value of the primary attribute, for a certain host and event type, as determined
17 the pattern algorithm using the mapping mechanism for mapping a plurality of attributes
18 including the primary attribute into an item for presentation, and the pattern algorithm
19 also determines if the newly arrived event, e.g., alarm, includes the attribute value for the
20 primary attribute, e.g., a certain host or a certain event type including SNMP request,
21 authentication failure, link up, link down, port up, port down, link down of host A, node
22 down of host B etc., shining the x-axis of the cross plot for the new time period so that the
23 new time period being presented on the x-axis covers the arrival time of the event and
24 plotting the event arrived within the shifted time period into the cross plot with the first
25 display label indicating the primary attribute. Ma discloses determining on the basis of
26 the recorded attribute values of event from the alarm log or the database whether or not
27 the newly arrived event for the new time period is part of the given pattern using the
28 pattern algorithm on the basis of a comparison of the attributes allocated to the given
29 pattern, for example a composite pattern of Page 13, on the basis of a comparison
30 analysis, and of the attribute assigned to the arrived event wherein the newly arrived
31 event are determined by the retrieval time ranges and data ranges including the host
32 names and types from the database, Ma further discloses determining if the newly arrived
33 event includes an attribute value of the given pattern including the mutual dependence
34 measurement of an m- pattern adding the event to the previous events being detected as
35 part of the given pattern, and redrawing all the events being associated with given
36 pattern in the cross plot by updating the cross plot.*

1 In response, the applicant respectfully take particular exception with the alleged equivalency of
2 elements in claims 2 and 3 and the cited art, and take exception with the Examiner assertions. This
3 is particularly so because of the amendment of claim 1. This is also in regard to use of words in
4 the claims attributes, primary, events, display label etc. The present invention in 2 and 3 is not
5 anticipated or made obvious by S. Ma, et al. As noted Ma's method is apparently that only one of
6 the event attributes may be plotted versus the arrival time of the events. Thus, the operators have
7 to switch continuously between the various event attributes to make sure that they do not miss a
8 significant event attribute or attributes or their simultaneous display. Ma is not concerned with the
9 'primary attribute' nor for a plurality of event attributes, as in claims 2 and 3. The addition of
10 Kranzlmuller apparently does nothing to make these obvious.

11 Also, the office communication states the visualizations are generated for any type of attribute, or
12 combination of several, recorded with the event data. A review of Ma and Kranzlmuller show that
13 the art still is concerned with data along a temporal axis. Thus, claims 2 and 3 are allowable over
14 Ma and Kranzlmuller in themselves and because each depends on allowable claim 1.

15 *Re Claims 4-5: Ma further discloses the third display label and the fourth display label
16 indicating the new patterns (See the three colored spikes in Fig. 6 and the four patterns
17 in Fig. 7). Ma discloses determining if the newly arrived event does not include an
18 attribute value of the given pattern, on the basis of the recorded attribute values of all
19 previous arrived events from the alarm logs or from the database, by means of the
20 mining algorithm whether or not the newly arrived event is part of a new pattern on the
21 basis of a comparison (Page 3) of the attributes allocated to the new pattern and of the
22 attributes assigned to the arrived events. Ma discloses allocating a third display label to
23 the events, including the coloring of the new pattern, indicating the attribute values of the
24 attributes being discovered as part of the new pattern wherein a large amount of patterns
25 can be discovered by the mining algorithms. Ma discloses plotting the all events being
26 detected by means of the mining algorithm as part of the new pattern into the cross plot
27 with the third display label indicating the new pattern, the position of the third display
28 label of each event in the cross plot being determined by the mapping algorithm (Page 12
29 for the mapping of the attributes into item and thereby determining the positions of the
30 patterns on the cross plot) on the basis of the attribute value of the attribute of the event
31 (event types, host names etc) being uncovered as part of the new pattern, such as SNMP
32 request) authentication failure, link up, link down, port up port down, link down of host
33 A, node down of host B etc, and its arrival time in the database, Ma discloses removing
34 all the events including an attribute value allocated to the primary attribute from the
35 cross plot, if a primary attribute to be presented with its attribute values on the y-axis of
36 the cross plot is changed (if the mapping mechanism for mapping a plurality of attributes*

1 *including the host names and event types are changed), allocating a fourth display label*
2 *including SNMP request, authentication failure, link up, link down, port up, port down,*
3 *link down of host A, node down of host B etc. to the events indicating the attribute values*
4 *of the new primary attribute (e.g., category attribute, event type of data objects). Ma*
5 *discloses plotting all the events arrived within the time period as retrieved from the*
6 *database and including an attribute value allocated to the new primary attribute into the*
7 *cross plot with the fourth display label, including SNMP request, authentication failure,*
8 *link up, link down, port up, port down, link down of host A, node down of host B etc.,*
9 *indicating the new primary attribute, such as the host name and event type, the position*
10 *of the fourth display label of each event in the cross plot being determined by the*
11 *mapping mechanism in Page 12 on the basis of the attribute value of the primary*
12 *attribute of the event and its arrival time as determined by the retrieval condition from*
13 *the database.*

14 In response, the applicant respectfully take particular exception with the alleged equivalency of
15 elements in claims 4 and 5 and the cited art, and take exception with the Examiner assertions.
16 This is in regard to use of words in the claims attributes, primary, events, display label etc. The
17 present invention in 4 and 5 is not anticipated or made obvious by S. Ma, et al. As noted,
18 applicants respectfully state that the indicating of new patterns in Ma, is not the steps of claim 4.
19 Ma and Kranzlmuller do not test as in claim 4, “if the newly arrived event does not include an
20 attribute value of the given pattern.” Nor do Ma and Kranzlmuller determine, “on the basis of the
21 recorded attribute values of all previous arrived events by means of the pattern algorithm whether
22 or not the newly arrived event is part of a new pattern on the basis of a comparison of the
23 attributes allocated to the new pattern and of the attributes assigned to the arrived events.” Nor
24 do Ma and Kranzlmuller test, “if the newly arrived event forms together with previous recorded
25 events the new pattern,” Nor do Ma and Kranzlmuller allocate, “a third display label to the events
26 indicating the attribute values of the attributes being uncovered as part of the new pattern.”
27 Certainly, Ma and Kranzlmuller does apparently not perform the step of, “plotting the all events
28 being detected by means of the pattern algorithm as part of the new pattern into the cross plot
29 with the third display label indicating the new pattern, the position of the third display label of
30 each event in the cross plot being determined by the mapping algorithm on the basis of the
31 attribute value of the attribute of the event being uncovered as part of the new pattern and its
32 arrival time.

1 Similarly, Ma with or without Kranzlmuller are not concerned with a ‘primary attribute nor with
2 the step of claim 5, of removing all the events including an attribute value allocated to the primary
3 attribute from the cross plot, if a primary attribute to be presented with its attribute values on the
4 y-axis of the cross plot is changed, allocating a fourth display label to the events indicating the
5 attribute values of the new primary attribute,” nor with the step of, “plotting all the events arrived
6 within the time period and including an attribute value allocated to the new primary attribute into
7 the cross plot with the fourth display label indicating the new primary attribute, the position of the
8 fourth display label of each event in the cross plot being determined on the basis of the attribute
9 value of the primary attribute of the event and its arrival time,” nor with the step of, “if a primary
10 attribute to be presented with its attribute values on the y-axis of the cross plot is changed,
11 allocating a fourth display label to the events indicating the attribute values of the new primary
12 attribute, and plotting all the events arrived within the time period and including an attribute value
13 allocated to the new primary attribute into the cross plot with the fourth display label indicating
14 the new primary attribute, the position of the fourth display label of each event in the cross plot
15 being determined on the basis of the attribute value of the primary attribute of the event and its
16 arrival time.

17 Also, for example, the office communication states "the application of data mining algorithms,
18 which are then used to generated multiple different visualizations. A review of Ma and
19 Kranzlmuller show that even the combination does not equal that generation of multiple
20 visualizations for cross-referencing. Thus claims 4 and 5 are allowable over Ma and Kranzlmuller
21 in themselves and because each depends on allowable claim 1.

22 *Re Claim 6: Ma further discloses the operator selects the events to be plotted and
23 displaying textual and coloring information associated with the selected events on the
24 event display (Page 4 and Figs. 6,7,9-10). Ma discloses plotting all attribute values,
25 including the attributes such as event type, link down, and host name, host A, in the
26 patterns marked as the link down of host A, node down of host B, recorded for an event,
27 as retrieved from the database, with the respective display label into the cross plot if the
28 event is selected by an operator and displaying textual information associated with the
29 selected event on the event display.*

1 In response, the applicant respectfully take particular exception with the alleged equivalency of
2 elements in claim 6 and the cited art, and take exception with the Examiner assertions.
3 In response, applicants respectfully state that exception is taken with the so called equivalencies
4 of elements in Claim 6 and the cited art. This is in regard to use of words in the claims attributes,
5 primary, events, display label etc. The present invention in claim 6 is not anticipated by S. Ma, et
6 al. As noted, applicants respectfully state that Ma is not concerned with the test and step of claim
7 6 of, "plotting all attribute values recorded for an event with the respective display label into the
8 cross plot if the event is selected by an operator, and displaying textual information associated
9 with the selected event on the event display.
10 Also, a review of Ma and Kranzlmuller show that the user has to guide the visualization manually.
11 Thus claim 6 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable
12 claim 1.

13 *Re Claim 7: Ma further discloses a pattern algorithm such as the data mining algorithm
14 suitable to perform multi-attribute pattern recognition (Figs. 6, 7, 9-10). Ma discloses
15 the mining algorithm being suitable to perform multi-attribute pattern recognition using
16 the mapping mechanism (Page 12) and the pattern comparisons/matching (Page 13).*

17 In response, the applicant respectfully take particular exception with the alleged equivalency of
18 elements in claim 7 and the cited art, and take exception with the Examiner assertions. The
19 present invention in claim 7 is not anticipated by S. Ma. There is apparently no indication that Ma
20 is concerned with multi-attribute pattern recognition or even any pattern recognition as in claim 7.
21 Being allegedly suitable is indeed not an anticipation of the invention in claim 7. Thus claim 7 is
22 allowable over Ma and Kranzlmuller for itself and because it depends on allowable claim 1.

23 *Re Claim 8: Ma further discloses using color such as Red and Green to color the pattern
24 Spikes and Pattern I, Pattern 2, Pattern 3, Pattern 4 for specific mark layouts (Figs.
25 6,7,9-10). Ma discloses each display label includes different colors marking the events.*

26 In response, the applicant respectfully take particular exception with the alleged equivalency of
27 elements in claim 8 and the cited art, and take exception with the Examiner assertions. A review
28 of Ma and Kranzlmuller show that even the combination does not have the elements as in claim 8.

1 Thus, claim 8 is allowable over Ma and Kranzlmuller for itself and because it depends on
2 allowable claim 1.

3 *Re Claim 9: Ma further discloses all events being uncovered as part of the pattern being
4 clustered by the display label such as Red Spikes, Green Spikes (Figs. 6,7 and 9-10). Ma
5 discloses all events being discovered as part of the pattern as clustered by the different
6 labels including Red Spikes and Green Spikes to indicate one of the plurality of events
7 such as SNMP request, authentication failure, link up, link down, port up, port down, link
8 dawn of host A, node down of host B etc indicating the new primary attribute.*

9 In response, the applicant respectfully take particular exception with the alleged equivalency of
10 elements in claim 9 and the cited art, and take exception with the Examiner assertions. There is
11 apparently no indication that Ma is at all concerned with clusters or clustering as in claim 9. Thus
12 claim 9 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable
13 claim 1.

14 *Re Claim 10: Ma further discloses a data mining algorithm and GUI (Page 14). Ma
15 discloses the mining algorithm carrying the steps as recited in the claim 1.*

16 In response, the applicant respectfully take particular exception with the alleged equivalency of
17 elements in claim 10 and the cited art, and take exception with the Examiner assertions. Claim 10
18 is amended herein. The response to claim 1 is appropriate to claim 10 which depends thereupon.
19 The program code is that of claim 1, which is not anticipated by Ma. Claim 10 is amended. Thus
20 claim 10 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable
21 claim 1.

22 *Re Claim 11: Ma further discloses the program code being stored on data carrier (see
23 page 5). Data carrier is inherent within the computer embodiment of Page 5.*

24 In response, the applicant respectfully take particular exception with the alleged equivalency of
25 elements in claim 11 and the cited art, and take exception with the Examiner assertions. Exception
26 is taken with the stated inherency. Claim 11 is amended herewith. There is apparently no
27 indication that Ma or Kranzlmuller discloses or is concerned with a data carrier as in claim 11.
28 Thus claim 11 is allowable over Ma and Kranzlmuller for itself and because it depends on
29 allowable claim 1.

1 *Re Claim 12: Ma further discloses an event visualization device for monitoring events in*
2 *a computer network (Page 3). The cited reference teach mapping a plurality of data*
3 *attributes to item to identify correlations across different hosts and event types by using*
4 *the mapping that maps the pair of event type and hart name to item and leaves key empty.*
5 *See Page 11, Moreover, the cited reference in Page 1, second paragraph, explicitly*
6 *teaches the attribute values, see the last paragraph of Page 6 and the first and second*
7 *paragraphs of Page 8, the last paragraph of Page 12, and the real data set collected*
8 *from a production computer network containing thousands of managed nodes including*
9 *routers; hubs and servers are described in the last paragraph of page 3 and identifying*
10 *unknown event patterns that can be used for real-time monitoring is described in the*
11 *second paragraph of page 3.*

12 In response, the applicant respectfully take particular exception with the alleged equivalency of
13 elements in claim 12 and the cited art, and take exception with the Examiner assertions. The
14 present invention in claim 12 is not anticipated by S. Ma. The response to claim 1 is appropriate
15 to claim 12, which depends thereupon. The device is for performing the steps of claim 1, which is
16 not anticipated by Ma. Thus claim 12 is allowable over Ma and Kranzlmuller for itself and
17 because it depends on allowable claim 1.

18 *Re Claims 13 and 15: Ma further discloses an implementation of the Event Miner*
19 *algorithm on the computer (Page 4-5).*

20 In response, the applicant respectfully take particular exception with the alleged equivalency of
21 elements in claims 13 and 15 and the cited art, and take exception with the Examiner assertions.
22 In response, applicants respectfully state that exception is taken with the so called equivalencies
23 of elements in Claims 13-16 and the cited art. The present invention in claim 13-15 are not
24 anticipated by S. Ma. The response to claim 1 is appropriate to claim 13 and 15, which depends
25 thereupon. Claim 14 is amended to be an independent claim of the Beauregard type, with all the
26 elements of claim 1. The implementations are for performing the steps of claim 1, which is not
27 anticipated by Ma. Thus claims 13-15 are allowable over Ma and Kranzlmuller for itself and
28 because it depends on, or has the matter, of allowable claim 1.

29 *Claim 14: The claim 14 is subject to the same rationale of rejection set forth in the claim*
30 *1.*

1 In response, the applicant respectfully take particular exception with the alleged equivalency of
2 elements in claim 14 and the cited art, and take exception with the Examiner assertions. Claim 14
3 is amended as in claim 1. Claim 14 now reads:

4 14. (Currently amended) A program storage device being a computer readable medium,
5 tangibly embodying a program of instructions executable by a computer to perform
6 method steps for monitoring network activities as a time-ordered sequence of events in a
7 computer network, each event having attributes triggered by an intrusion-detection
8 system, each event being characterized by a given set of attributes called dimensions, each
9 event forming an n-dimensional space, said step of monitoring comprising the steps of:

10 said computer network triggering said events, each event being provided with attribute
11 values allocated to a given set of attributes of said each event, each attribute having a
12 particular attribute value,

13 simultaneously monitoring each particular attribute value of various event attributes from
14 said given set of attributes versus the arrival time of said each event,

15 providing an event display with a cross plot having x and y coordinate axes, the x-axis
16 presenting a time period and the y-axis presenting an attribute value range, and visualizing
17 data along said x and y coordinate axes, said axes being attribute axes,

18 determining a primary attribute of said each event selected from the given set of attributes,
19 each said primary attribute of said each event to be presented with its a corresponding
20 attribute values value on the y-axis of the cross plot,

21
22 allocating a first display label to the events indicating the attribute values value of the
23 primary attribute of each event providing a pattern algorithm to detect whether an arrived
24 event is part of the given pattern on the basis of a comparison of the attributes allocated to
25 the given pattern and of the attributes assigned to the arrived event, providing a mapping

1 algorithm to map any attribute value of an attribute selected from the given set of
2 attributes onto the y-axis of the cross plot,

3 allocating a second display label to said each event indicating the attribute values of the
4 attributes being uncovered as part of the given pattern,

5 plotting all events that arrived within the time period and including an attribute value
6 allocated to the primary attribute into the cross plot with the first display label indicating
7 the primary attribute, the position of the first display label of said each event in the cross
8 plot being determined on the basis of the attribute value of the primary attribute of the
9 event and its arrival time,

10 plotting all events that arrived within the time period and being detected by means of the
11 pattern algorithm as part of the given pattern into the cross plot with the second display
12 label indicating the given pattern, the position of the second display label of said each
13 event in the cross plot being determined by the mapping algorithm on the basis of the
14 attribute value of the attribute of the event being uncovered as part of the given pattern
15 and its arrival time, and

16 viewing a secondary attribute of said each event together with the primary attribute on
17 said display.

18 Thus, the entire response to claim 1 is appropriate to amended claim 14. Thus claim 14 is
19 allowable over the combined art of Kranzlmuller and Ma.

20 *Claim 16: The claim 16 is subject to the same rationale of rejection set forth in the*
21 *claims 2-4,*

22 In response, the applicant respectfully take particular exception with the alleged equivalency of
23 elements in claim 16 and the cited art, and take exception with the Examiner assertions. There is
24 apparently no indication that Ma and Kranzlmuller perform the added steps of claim 16. The

1 present invention in claim 16 is not anticipated by S. Ma. The response to claim 1 is appropriate
2 to claim 16, which depends thereupon. The method is for performing more steps over the steps
3 of claim 1, which is not anticipated by Ma. Thus claim 16 is allowable over Ma and Kranzlmuller
4 for itself and because it depends on allowable claim 1.

5 *Claim 17: The claim 17 is subject to the same rationale of rejection set forth in the claim*
6 *5.*

7 In response, applicants respectfully state that as with claim 5 exception is taken with the so called
8 equivalencies of elements in Claim 17 and the cited art. This is in regard to use of words in the
9 claims attributes, primary, events, display label etc. There is apparently no indication that Ma and
10 Kranzlmuller perform the added steps of claim 17. The present invention in claim 17 is not
11 anticipated by S. Ma. The response to claim 1 is appropriate to claim 17, which depends
12 thereupon. The method is for performing more steps over the steps of claim 16, which is not
13 anticipated by Ma. Thus claim 17 is allowable over Ma and Kranzlmuller for itself and because it
14 depends on allowable claim 1.

15 *Claim 18: The claim 18 is subject to the same rationale of rejection set forth in the*
16 *claims 2-4.*

17 In response, applicants respectfully state that as with claims 2-4, exception is taken with the so
18 called equivalencies of elements in Claim 18 and the cited art. This is in regard to use of words in
19 the claims attributes, primary, events, display label etc. There is apparently no indication that Ma
20 and Kranzlmuller has the added elements of claim 18. The present invention in claim 18 is not
21 anticipated by S. Ma. The response to claim 1 is appropriate to claim 18, which depends
22 thereupon. The device is for more elements than claim 5, which is not anticipated by Ma. Thus
23 claim 18 is allowable over Ma and Kranzlmuller for itself and because it depends on allowable
24 claim 1.

25 *Claim 19: The claim 19 is subject to the same rationale of rejection set forth in the claim*
26 *5.*

1 In response, applicants respectfully state that as with claim 5 exception is taken with the so called
2 equivalencies of elements in Claim 19 and the cited art. This is in regard to use of words in the
3 claims attributes, primary, events, display label etc. There is apparently no indication that Ma and
4 Kranzlmuller perform the added steps of claim 19 has the added elements of claim 189. The
5 response to claim 1 is appropriate to claim 17, which depends thereupon. The device is for more
6 elements than claim 5, which is not anticipated by Ma. Thus claim 17 is allowable over Ma and
7 Kranzlmuller for itself and because it depends on allowable claim 1.

8 *Claim 20: The claim 20 is subject to the same rationale of rejection set forth in the claim*
9 *1.*

10 In response, the applicant respectfully take particular exception with the alleged equivalency of
11 elements in claim 20 and the cited art, and take exception with the Examiner assertions. Claim 20
12 is amended herein, and now reads:

13 20. An article of manufacture comprising apparatus for monitoring events in a computer
14 network, the apparatus comprising:

15 said computer network having means for intrusion-detection triggering said events, each
16 event having attributes triggered by the means for intrusion-detection, each event being
17 characterized by a given set of attributes called dimensions, each event forming an
18 n-dimensional space, each event being provided with attribute values allocated to a given
19 set of attributes of said each event,

20 means for simultaneously monitoring various event attributes from said given set of
21 attributes versus the arrival time of said each event,

22 means for providing an event display with a cross plot having x and y coordinate axes, the
23 x-axis presenting a time period and the y-axis presenting an attribute value range, and
24 visualizing data along said x and y coordinate axes, said axes being attribute axes,

1 means for determining a primary attribute of said each event, said primary attribute being
2 selected from the given set of attributes, each said primary attribute of said each event to
3 be presented with a corresponding attribute value on the y-axis of the cross plot,

4
5 means for allocating a first display label to the events indicating the attribute value of the
6 primary attribute of each event, providing a pattern algorithm to detect whether an arrived
7 event is part of the given pattern on the basis of a comparison of the attributes allocated to
8 the given pattern and of the attributes assigned to the arrived event, providing a mapping
9 algorithm to map any attribute value of an attribute selected from the given set of
10 attributes onto the y-axis of the cross plot,

11 means for allocating a second display label to said each event indicating the attribute
12 values of the attributes being uncovered as part of the given pattern,

13 means for plotting all events that arrived within the time period and including an attribute
14 value allocated to the primary attribute into the cross plot with the first display label
15 indicating the primary attribute, the position of the first display label of said each event in
16 the cross plot being determined on the basis of the attribute value of the primary attribute
17 of the event and its arrival time,

18 means for plotting all events that arrived within the time period and being detected by
19 means of the pattern algorithm as part of the given pattern into the cross plot with the
20 second display label indicating the given pattern, the position of the second display label of
21 said each event in the cross plot being determined by the mapping algorithm on the basis
22 of the attribute value of the attribute of the event being uncovered as part of the given
23 pattern and its arrival time, and

24 means for viewing a secondary attribute of said each event together with the primary
25 attribute on said display.

1 As described with regard to claim 1, claim 20 shows that it is in regard to intrusion-detection.
2 Also, in claim 20, the attributes are event attributes, and to show explicitly that it includes “means
3 for simultaneously monitoring various event attributes versus the arrival time of each the events,”
4 and to specifically include “means for viewing a secondary attribute of said each event together
5 with the primary attribute on said display.” This apparently more clearly distinguishes claim 1 and
6 20, from the cited reference. Thus claim 20 is allowable over Ma and Kranzlmuller.

7 It is anticipated that this amendment brings the application to allowance of claims 1-20.
8 Favorable action is respectfully solicited. In the unlikely event that any claim remains rejected,
9 please contact the undersigned as required by the MPEP, by phone in order to discuss the
10 application.

11 Please charge any fee necessary to enter this paper to deposit account 50-0510.

12 Respectfully submitted,

13 By: _____/Louis Herzberg/ _____
14 Dr. Louis P. Herzberg
15 Reg. No. 41,500
16 Voice Tel. (845) 352-3194
17 Fax. (845) 352-3194
18 3 Cloverdale Lane
19 Monsey, NY 10952

20 Customer Number: 54856